Закон о безопасности потенциально опасен?

Федеральный закон от 06.07.2016 N 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности», именуемый в общественных дискуссиях «законом Яровой» — в честь одного из его авторов, — наделал немало шума. В частности, из-за поправок в Закон «Об информации, информационных технологиях и защите информации».

Роман Васильев
Дмитрий Лашин

Но для большинства людей так и осталось непонятно, о чем был спор. Ни авторы закона не поделились своим представлением, как им видится его исполнение, ни критики толком не объяснили, почему, по их мнению, этот закон не может быть реализован. Давайте попробуем разобраться и начнем с самого начала. Для этого нам необходимо обратиться к ряду технических терминов, в частности — шифрованию.

Шифрование — это некое преобразование (последовательность действий, алгоритм) исходных данных в «неразбериху», из которой при помощи другого преобразования (расшифрование) опять можно получить первоначальные данные. При этих преобразованиях используется некое значение, которое называется ключом или секретом. Простейший пример — подстановка, когда каждый символ начальных данных заменяется на другой, ему соответствующий, как это описано в известном рассказе о Шерлоке Холмсе «Пляшущие человечки».

Шифры, которые при зашифровывании и расшифровывании используют один и тот же ключ, называют симметричными. Если же при расшифровывании используется отличный ключ от ключа зашифровывания, то такой шифр называется асимметричным. При асимметричном шифровании знание одного из ключей, который называется «открытым», не позволяет вычислить второй — «закрытый». На этом принципе построена, например, цифровая подпись: только вам известен закрытый ключ, поэтому те сообщения (документы), которые могут быть получены при расшифровании с применением опубликованного вами открытого ключа, можно смело считать непросто точно вашими, но еще и подписанными вами.

Главной проблемой при симметричном шифровании является передача и хранение ключа между пользователями. Одним из наиболее распространенных алгоритмов симметричного шифра на сегодняявляется AES (Advanced Encryption Standard), алгоритм которого на аппаратном уровне реализован в последних версиях процессоров Intel. Асимметричные алгоритмы более сложные, а значит, требуют больше времени при шифровании и оперируют более длинными ключами.

Теперь давайте разберемся, как происходит применение шифрования при обмене данными между различными устройствами. Явно мы с этим сталкиваемся, когда проводим оплату банковской карточкой своей покупки в Интернете. Обычно нам выдается сообщение, что передача данных нашей банковской карточки будет проходить по защищенному каналу. Что это значит? На сегодня общепринятым стандартом является TLS-протокол, обеспечивающий безопасную передачу данных в Интернете. Упрощенно протокол выглядит так. Сначала ваш компьютер получает от сайта банка (или компании, обеспечивающей оплату) открытый ключ и с его помощью зашифровывает случайную последовательность символов. Эта последовательность называется сеансовым ключом и в дальнейшем будет использоваться как ключ уже в другом симметричном алгоритме. Зашифрованный сеансовый ключ передается сайту банка, тот его расшифровывает, и потом обмен данными уже происходит с использованием симметричного шифрования с применением сеансового ключа. При окончании обмена данными (разрыве связи) сеансовый ключ уничтожается.

Получается, что вот этот сеансовый ключ, по новому закону, и должен передаваться «организатором распространения информации» правоохранительным органам. Под «организатором распространения информации» понимается любой ресурс, где можно обмениваться электронными сообщениями. Хорошо если этот «организатор» сам является участником обмена данными. А как быть, например, популярным мессенджерам Viber и WhatsApp? Ключи создаются и хранятся только на устройствах пользователей, а у самих «организаторов» их нет.

В Казахстане эту проблему решили так: при установлении защищенного соединения по протоколу TLS открытый ключ сервера получается не напрямую от сервера, а от достоверного источника — Сертификационного центра, с которым браузер пользователя может сам установить защищенное соединение (адрес Сертификационного центра и его открытый ключ уже зашиты в код браузера). Ввиду того что в Казахстане провайдером является государственный монополист Казахтелеком, весь трафик проходит через него. Таким образом, провайдер имеет возможность при обращении пользователя в Сертификационный центр блокировать его доступ и вместо истинного ключа сервера подставлять свой, соответствующий «национальным стандартам», а затем перешифровывать весь трафик между пользователем и сервером, при этом имея возможность прослушивать его. Для реализации такого способа подмены сертификатов Казахтелекому не требуется создание дата-центров для хранения переданного трафика, как это теперь должны будут делать «организаторы» в России. Возможно, этим озадачат Комитет национальной безопасности Казахстана. Время покажет.

Касательно реализации предусмотренного в Российской Федерации порядка передачи ключей шифрования в адрес уполномоченного органа в области обеспечения безопасности Российской Федерации возникает масса вопросов. Вероятно, будет разработан некий локальный (российский) стандарт. Но как в таком случае будут работать устройства наших зарубежных гостей?

Также нельзя исключать, что западные компании, не согласные применять данный стандарт, будут вынуждены уйти из России, а мы сможем общаться только внутри страны.

Но самое опасное — это то, что реализация данного закона ведет к увеличению киберугроз. Как уже отмечалось, главной проблемой при обычном симметричном шифровании является передача и сохранение ключа в тайне. Теперь этот ключ вместе с данными будет храниться где-то на сайте, посредством которого вы обменивались сообщениями, а потом и в правоохранительных органах. Значит, появляется еще как минимум два источника (две потенциальные возможности), где злоумышленник может попытаться получить доступ к интересующим его данным.

Закон принят, но как он будет работать, на данный момент сказать трудно. Остается только смотреть и наблюдать, как будут развиваться события. ■